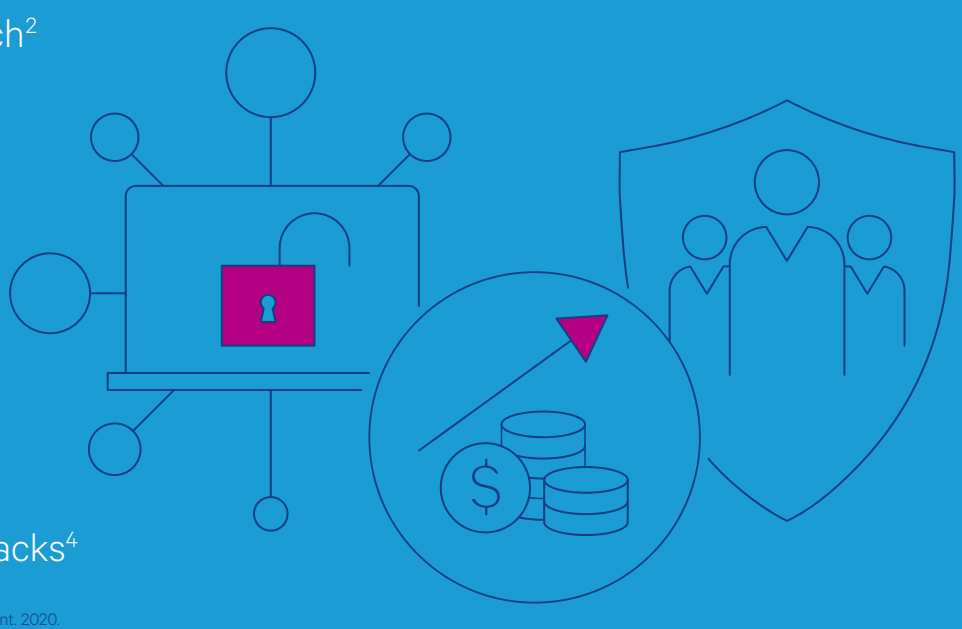
CYBERSECURITY IN PARTNERSHIP

A malicious hacking attack takes place every 39 seconds,[1] making cybersecurity a growing concern for global governments and businesses. Yet, it's not easy to secure your organisation in a complex threat landscape in which attacks are increasing in both frequency and sophistication.

USD 3.86M
average cost per data breach[2]

2,244
cyber attacks per day[3]

78%
increase in supply chain attacks[4]



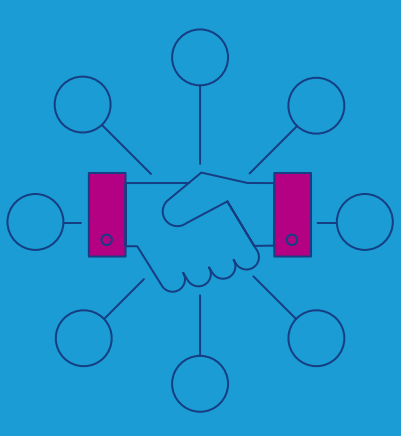
1 10 Facts About Supply Chain Risk You Need To See. ID Agent. 2020.
2 Cost of a Data Breach Report. IBM. 2020.
3 Study: Hackers Attack Every 39 Seconds. University of Maryland. 2007.
4 10 Facts About Supply Chain Risk You Need To See. ID Agent. 2020.

CYBERSECURITY AS A SHARED RESPONSIBILITY

Cyber-attacks can have devastating consequences. With supply chain attacks, for example, threat actors seek out the weakest link in a supply chain to ultimately infiltrate the systems of the target organisation. That's why it's increasingly important to work with suppliers and partners that will align with you on cybersecurity standards and requirements. At SES, we see cybersecurity as a collective responsibility and ensure that our chosen partners share this view, so that the services you receive are trustworthy.

RESILIENT INFORMATION SECURITY PROGRAMME

We regularly review and update our information security policies to keep your data protected and confidential.

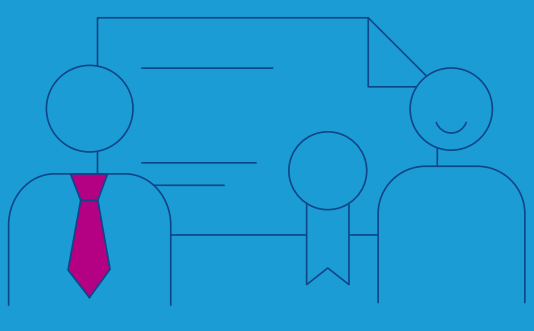


CLEARLY DEFINED RESPONSIBILITIES

We define and agree upon security responsibilities early in our partnerships with the intention of building a collective defence against cyber threats.

ALIGNMENT ON STANDARDS

We implement diligent security standards and practices that enable us to bring you secure services and meet your evolving cybersecurity requirements.



SIMPLIFYING BUSINESS PARTNERSHIPS

A shared approach to cybersecurity is central to building strong partnerships. As the cyber threat landscape changes, organisations need to adapt their information security approach, keeping partnership in mind. Our information security programme is based on industry best practices and meets the security requirements of each market segment we serve.

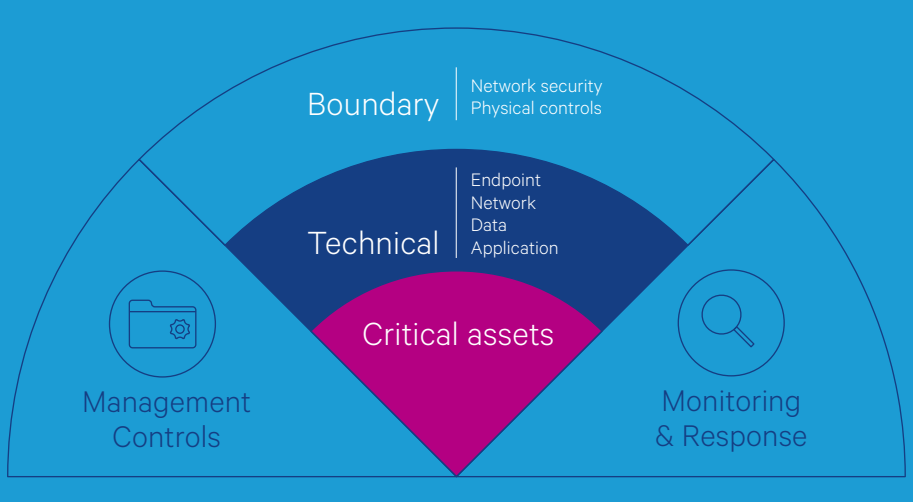
COMPLIANCE WITH INTERNATIONAL SECURITY STANDARDS

Some of our services are already ISO 27001 certified, and we aim to enhance and extend the scope of this certification in the future. We are also in the process of preparing to qualify for the IA-Pre certification to meet US Department of Defense requirements.

LEADS THE SPACE INDUSTRY

To better share information security responsibilities with our partners and customers, we take the initiative to help set security standards for our industry. As a founder of the Space ISAC, we're helping drive standardisation across the space industry.

ENABLING SCALABILITY



At SES, we follow a defense in depth (DiD) approach to secure our operations by implementing controls in multiple layers, and therefore, reducing the likelihood of a single point of failure carrying through to the whole system. This approach, combined with our commitment to developing partnerships that share our responsibility towards cybersecurity, allows us to help you scale your business securely and reliably.

1 | BOUNDARY LAYER

All our physical locations meet strict security standards, and our network is protected via multiple layers of security controls.

2 | TECHNICAL LAYER

Technical controls in multiple sub-layers across several areas—including our internal network, critical applications, endpoints, and data.

3 | MANAGEMENT CONTROLS

A series of management controls covering a broad range of security elements ensures continuous improvement of our information security management system.

4 | MONITORING AND RESPONSE

A state-of-the-art Security Information and Event Management (SIEM) platform ensures a continuous process to identify, manage, record, and analyse active threats.

PARTNERS IN SECURITY, PARTNERS IN BUSINESS

The best way to reduce the likelihood of your organisation being compromised is to have a common approach to cybersecurity in your partnerships. By working with suppliers and partners that proactively adopt industry best practices and standards, and view cybersecurity as a shared responsibility, you can navigate and respond to the evolving cyber threat landscape more easily—simplifying the way you work and grow together.

Learn more about
CYBERSECURITY IN PARTNERSHIP
Download the guide now >

SES